AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior version, and listings, of claims in the application.

Listing of Claims:

Claim 1 (Currently Amended): A secure key replacement (SKR) method executed on a suitably programmed device, comprising:

receiving a rekey request, wherein the rekey request identifies a private key for replacement, the rekey request, comprising:

a SKR key, and

a challenge;

authenticating the rekey request;

replacing the identified private key with the SKR key;

signing the challenge with the SKR key; ~~and~~

returning the signed challenge; and

preventing a replay attack, comprising:

storing key identifiers of previously deleted private keys in memory,

reading a key identifier of the private key,

comparing the read key identifier to the key identifiers of previously deleted private keys, and

rejecting the key request if the read key identifier matches any of the key identifiers of previously deleted keys.

Claim 2 (Previously Presented): The secure key replacement method of claim 1, wherein the rekey request is received at a removable device.

Claim 3 (Previously Presented): The secure key replacement method of claim 2, wherein the removable device comprises one of a magnetic card, a smart card, and a token.

Claim 4 (Previously Presented): The secure key replacement method of claim 2, wherein the

removable device is coupled to a user's computer.

Claim 5 (Previously Presented): The secure key replacement method of claim 1, wherein the rekey request is received at a user's computer.

Claim 6 (Previously Presented): The secure key replacement method of claim 1, further comprising deleting the identified private key.

Claim 7 (Canceled)

Claim 8 (Currently Amended): The secure key replacement method of claim ~~7~~, 1 wherein preventing a replay attack, comprises:

determining a time stamp on the rekey request;

comparing the time stamp to a current time; and

rejecting the rekey request when the time stamp differs from the current time by a specified limit.

Claim 9 (Previously Presented): The secure key replacement method of claim 8, wherein the specified limit is 24 hours.

Claim 10 (Canceled)

Claim 11 (Previously Presented): The secure key replacement method of claim 1, wherein receiving the rekey request comprises receiving the key request from a certificate authority, and wherein returning the signed challenge comprises returning the signed challenge to the certificate authority.

Claim 12 (Previously Presented): The secure key replacement method of claim 11, wherein the certificate authority is located at an Internet web site.

Claim 13 (Previously Presented): The secure key replacement method of claim 1, wherein authenticating the key request comprises checking a digital signature of the key request.

Claim 14 (Previously Presented): The secure key replacement method of claim 1, wherein the private key allows access to one or more documents.

Claim 15 (Previously Presented): The secure key replacement method of claim 1, wherein the private key allows execution of transactions comprising one of on-line banking, on-line purchasing, and viewing web site content.

Claim 16 (Currently Amended): A method, executed by a suitably programmed device, for secure replacement of private keys, comprising:

sending a rekey request to a user terminal, the rekey request comprising:

identifiers of one or more private keys to be replaced,

secure key replacement protocol (SKRP) keys to replace the private keys, and

a challenge to be signed at the user terminal, wherein a private key is replaced with a SKRP key and wherein the challenge is signed with the SKRP key; ~~and~~

receiving the signed challenge; and

preventing a replay attack, comprising:

storing key identifiers of previously deleted private keys in memory,

reading a key identifier of the private key,

comparing the read key identifier to the key identifiers of previously deleted private keys, and

rejecting the key request if the read key identifier matches any of the key identifiers of previously deleted keys.

Claim 17 (Original): The method of claim 16, wherein the rekey request further comprises a time stamp, wherein the time stamp is compared to a current time at the user terminal.

Claim 18 (Original): The method of claim 16, wherein sending the rekey request comprises sending the rekey request from an Internet web site.

Claim 19 (Original): The method of claim 16, wherein the user terminal is a node on a computer network, and wherein sending the rekey request comprises sending the rekey request from another node on the computer network.

Claim 20 (Original): The method of claim 16, wherein the private keys are stored on a removable device, the removable device adapted for insertion into the user terminal, further comprising receiving an indication from the user terminal when the removable device is inserted into the user terminal.

Claim 21 (Currently Amended): An apparatus comprising computing devices having programming that provides secure key replacement (SKR), the programming comprising:

a receiving module that receives and processes a SKR request, the SKR request comprising:

an identity of a private key to be replaced,

a SKR key to replace the private key, and

a challenge that, when signed, indicates the private key is replaced with the SKR key;

an authentication module that checks authenticity of the SKR request; a rekey module that replaces the private key with the SKR key and signs the challenge; ~~and~~

a return module that returns the signed challenge; and

prevention means to prevent a replay attack, comprising:

a memory that stores identities of previously deleted private keys, and

a program that compares the identity of the private key to be replaced with the identities of the previously deleted private keys and rejects the SKR request if the identity of the private key to be replaced matches any of the identities of the previously deleted keys.

Claim 22 (Canceled)

Claim 23 (Currently Amended): The apparatus of claim ~~22~~, 21, wherein the SKR request further comprises a time stamp indicative of a time of issuance of the SKR request, and wherein the prevention means, comprises:

a program, operable to read the time stamp on the SKR request and to compare the time stamp to a current time.

Claim 24 (Canceled)

Claim 25 (Original): The apparatus of claim 21, wherein the receiving module, the authentication module, the rekey module and the return module are implemented on a removable device capable of insertion into a user terminal.

Claim 26 (Original): The apparatus of claim 25, wherein the removable device is one of a magnetic card, a smart card, and a token.

Claim 27 (Original): The apparatus of claim 25, wherein the user terminal is a computer operating in a communications network, and wherein the SKR request is provided by a certificate authority coupled to the communications network.